(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 November 2002 (07.11.2002)

PCT

(10) International Publication Number
WO 02/089442 A1

(51) International Patent Classification[7]: H04L 29/06, G06F 17/60, 17/30

(21) International Application Number: PCT/EP01/08292

(22) International Filing Date: 18 July 2001 (18.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/287,015 30 April 2001 (30.04.2001) US

(71) Applicant: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventors: **DURAN, Julian**; 151 Calderon Avenue #242, Mountain View, CA 94041 (US). **ARNBERG, Tommy**; Itaranta 3 B 15, FIN-02110 Espoo (FI).

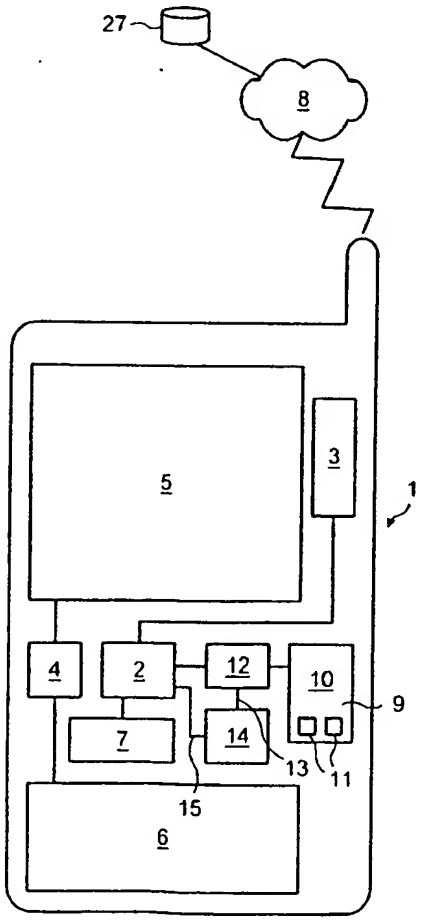
(74) Agents: **JOHNSON, Ian** et al.; Nokia IPR Department, Nokia House, Summit Avenue, Farnborough, Hampshire GU14 0NG (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK (utility model), SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,

[Continued on next page]

(54) Title: IMPROVEMENTS IN AND RELATING TO CONTENT DELIVERY



(57) Abstract: A system for delivering content to a terminal includes a secure content server (27). The server (27) includes a database in which content delivery conditions are defined. At least one of the delivery conditions relates to a location at which it is permissible to render content. A request from a terminal (1) to deliver content for rendering will be accepted provided the terminal (1) is determined to be within the pre-defined location.

WO 02/089442 A1

IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *with international search report*

Improvements in and relating to content delivery

The present invention relates to the delivery of content, particularly, although not exclusively, to mobile terminals.

Traditionally, the distribution of content, whether it is audio, video, textual or similar matter has been controlled by the right holder. Thus, a right holder has been able to release content in a format and at a time of their choice. In addition, the right holder has been able to license the distribution of content through collecting societies and the like particularly in relation to public performance of content such as audio and visual works. A licence to permit such performances is typically made available through a collection society or body which collectively negotiates licence terms on behalf of its members, the right holders. Such licences may restrict the time, location and other conditions under which the content is made available.

In addition to the market conditions which may influence the release of content, the right holder may also have to comply with local legislation dictating the availability of content to users. For example, content may be made available to a user only above a certain age.

More recently, right holders have had to adapt to new forms of distribution such as digital media in the form of compact discs (CDs), digital versatile discs (DVDs) as well the possibility of distribution over networks such as the Internet. Some efforts have been made to maintain the ability of the right holder to control the distribution of content and include the concept of regional coding applied to DVDs, for example. As a result of such coding, a DVD may be rendered by a compliant player only, that is a player having a corresponding regional code.

Thus, according to one aspect of the invention, there is provided a content delivery system for securely rendering content on a terminal, the system comprising a mobile terminal operable to establish a connection to a network and request delivery of content from a secure content server, said network being operable to determine the location of said terminal and provide access to said secure content server, the server being operable to associate said content identified in said request with at least one delivery condition stored on a database, a said at least one delivery condition defining a rendering location, the server being further operable to obtain the location of the terminal from said network such that where said terminal location corresponds to said rendering location content is delivered to said terminal.

In addition to allowing the right holder to control the distribution of her digital content in a manner that has become customary, an audit server may integrated with the system such that access to the content may be monitored. Although content may be rendered by the terminal itself, it would be possible to deliver content to a standalone rendering machine provided the server could be assured that the machine is both authenticated and located within an area meeting the delivery condition. Advantageously, the system allows for differentiation of delivery conditions such that content may be stored centrally but access to that content via a network is controlled to meet local legislative requirements, thus the content provider is able to make content available digitally relying on local controls within secure servers on networks to which terminals have access.

According to another aspect of the invention, there is provided a content delivery system for securely rendering content on a terminal, the system comprising a mobile terminal operable to determine its location and to establish a connection to an access point in order to request delivery of content from a secure content server, said access point being operable to provide access to said secure content server, the server being operable to associate said content identified in said request with at least one delivery

condition stored on a database, a said at least one delivery condition defining a rendering location, the server being further operable to obtain the location of the terminal from said access point such that where said terminal location corresponds to said rendering location content is delivered to said terminal.

Conveniently, the terminal includes a positioning system such as GPS, the output of which is trusted. Consequently, there is no need for the network operator to provide location-determining capability. Such a system may find favour in those networks where terminal positioning is already a requirement.

According to a further aspect of the invention, there is provided a content delivery system for securely rendering content on a terminal, the system comprising a mobile terminal operable to determine its location and to establish a connection to an access point in order to request delivery of content from a secure content server, said access point being operable to provide access to said secure content server, the server being operable to associate said content identified in said request with at least one delivery condition stored on a database, a said at least one delivery condition defining a rendering location, the server being further operable to obtain the location of the terminal from said access point such that where said terminal location corresponds to said rendering location content is delivered to said terminal.

Advantageously, the system may be scaled to meet the requirements of different networks, thus an access point may be provided by a base station of a public land mobile network (PLMN), a Local Area Network (LAN), a Wireless Local Area Network, or even a point to point connection utilising Low Power Radio Frequency or Infrared, for example. Clearly, the delivery route for the content need not be the same as that used to request the content. Thus, a terminal may need to operate in a number of communication modes.

According to yet another aspect of the invention, there is provided a content delivery system for securely rendering content on a terminal, the system

comprising a mobile terminal operable to determine its location and to establish a connection to an access point in order to request delivery of content from a secure content server, said access point being operable to provide access to said secure content server, the server being operable to associate said content identified in said request with at least one delivery condition stored on a database, a said at least one delivery condition defining a rendering location, the server being further operable to obtain the location of the terminal from said terminal such that where said terminal location corresponds to said rendering location content is delivered to said terminal.

According to a still further aspect of the invention, there is provided a secure content server including a database having stored thereon at least one delivery condition associated with content, the server being operable in response to a request for content from a terminal to determine from said database a said at least one delivery condition defining a rendering location of said content, the server being further operable to obtain the location of the terminal such that where said terminal location corresponds to said rendering location said content is delivered to said terminal.

The server may from part of a network architecture through via which the content is delivered to the terminal, in which case the delivery conditions may be set, at least in part, by the network operator to meet with local legislative requirements regarding accessibility to content. Advantageously, such a server could form part of a private network such as an intranet, whereby content is available for rendering only within areas defined by the intranet operator. Thus, an organisation may restrict the availability of content such as text, charts, sounds, music and other data to its premises.

According to a another aspect of the invention, there is provided a content delivery method for securely rendering content on a terminal, the method comprising receiving a request from a terminal for delivery of content, associating said content identified in said request with at least one delivery

condition stored on a database, a said at least one delivery condition defining a rendering location, obtaining the location of the terminal and delivering said content to said terminal where said terminal location corresponds to said rendering location.

In order to understand the present invention more fully, a number of embodiments thereof will now be described by way of example and with reference to the accompanying drawings, in which:

Figure 1 is a block diagram illustrating a personal trusted device forming part of a system according to the present invention;

Figure 2 is a schematic diagram illustrating a number of embodiments the system of Figure 1; and

Figure 3 is schematic diagram illustrating the data structure utilised in the system of Figure 1.

Referring to Figure 1, there is shown a Personal Trusted Device (PTD) 1 which includes the functionality of a mobile terminal as is well known to those skilled in the art. Thus, the PTD 1 includes a controller 2 having connections to a transceiver 3, a user interface 4, having further connections to a display 5 and keypad 6, and a memory 7, the operation of which, in relation to a wireless network 8, are well understood by those skilled in the art.

In addition to the known functionality of a mobile terminal, the PTD 1 also includes a protected database 9 within a tamperproof module 10. As will be described in more detail below, the database 9 facilitates the storage of digital rights information or vouchers 11. The vouchers relate to content held in secure storage. Access to the database 9 is restricted to a digital rights management engine 12, which also interfaces with the controller 2. A secure output connection 13 from the digital rights management engine 12 is provided to a rendering machine 14 having an output connection 15 to the controller 2.

Referring to Figure 2, within the coverage area of the network 8 there are a plurality of so-called hotspots **A**, **B** **C** and **D** served by at least one base station 17. Of these hotspots **A** and **B** are co-located with a fast-food restaurant 18 and shopping mall 19 respectively, whilst **C** and **D** correspond to the location of a doctor's surgery 20 and her patient 21, respectively. The physical location of each hotspot is defined in suitable terms and may be held in an appropriate database 23 of which there may be more than one. Thus, the fast-food restaurant 18 includes a pico-cellular base station 24 providing coverage to the immediate surroundings, namely the interior of the restaurant 18. The network address of the base station 24 is held in a location database or Home Location Register (HLR) 23a forming an element of the network 8. In the case of the shopping mall 19, the geographical co-ordinates of the mall 19 are stored in a location database 23b connected to the Internet 16 and maintained by an Internet Service Provider (ISP) 25. The doctor's surgery 20 includes a Low Power Radio Frequency (LPRF) access point 26, connected to a patient database 23c forming part of a surgery management system. The patient's 21 location is determined by a PTD 1 under the control of and in the possession of the patient 21, which PTD 1 further includes LPRF connectivity 26.

Secure content storage 27 is provided in a plurality of appropriate locations. Thus, medical records may be stored securely on a content server 27c forming part of the surgery management system. Other content may be stored within a secure content server 27a on the network 8 or even on a secure content server 27b connected directly to the Internet 16.

With reference to Figure 3, within the secure content storage 27 a record 28 exists for each content item 29. In addition to a field 30 identifying the corresponding content item 29, The record 28 includes a field 31 identifying a set of locations or a pointer to an external location database holding location information at which the content 29, to which the record relates, may be

rendered. Typically, the content 29 comprises a header portion 32 including data 33 to which the identifying field 30 of the record 28 points and a payload portion 34. Optionally, the record 28 includes a further field 35 indicating at what times and/or for how long the content 29 to which it relates may be rendered. Further fields 36 containing data addressing the needs of local legislation, such as age restrictions and the like, may also be provided. In a non-illustrated embodiment, rather than provide a separate record for each item of content, metadata associated with the content itself contains the restrictions, if any, imposed on rendering thereof.

Referring particularly to Figures 1 and 3, a user downloads or otherwise obtains a voucher 11 pertaining to content 29 which she may subsequently wish to render on her PTD 1. Thus, in response to a request generated via the UI 4 of her PTD and passed by the controller 2 to the digital rights management engine 12, the engine 12 obtains a URL from the voucher 11. The URL provides an address of a secure content server 27 holding the content 29 to which the voucher 11 pertains. The controller 2 having first established a communications channel over the network 8, passes the request to the secure content server 27 together with data indicative of whether the PTD 1 is capable of providing trusted information identifying its physical location.

The server 27 receives the request and commences a handshaking process with the engine 12 contained within the PTD 1. The engine 12 utilises the Public Key Infrastructure (PKI) including those elements held within the voucher 11, namely private keys, to authenticate the voucher 11 and hence the request. If the server is unable to authenticate the voucher 11 then the session is terminated.

Following authentication of the voucher 11, the secure content server 27 seeks to validate the conditions for delivery of the content 29 to the PTD 1 for rendering. The server 27 determines from data provided with the request

whether the PTD 1 is capable of providing trusted location information. The server then accesses the record 28 corresponding to the content 29 to be rendered and determines firstly, what limitation if any is placed on a rendering location for the content 29. In the event that such a limitation exists, the server 27 field determines in what terms the limitation is defined. Thus, the limitation could be defined in relation to a network, elements of a network, geographical co-ordinates or proximity to another device, for example. Depending on the nature of the location defined in the field 31, the server 27 will adopt a different approach to determining the location of the PTD 1. Clearly, if the location is defined in terms of geographical co-ordinates, then a PTD 1 with the capability to provided trusted location information can be interrogated by the server 27 and geographical co-ordinates provided thereto. If no such facility exists or the facility is unavailable, perhaps the PTD 1 is within a building or other structure, then a network 8 based technique such as base station triangulation may be used to attempt to locate the PTD 1.

Where the location is defined by reference to the network 8 architecture with which a PTD 1 is associated, such as by proximity to a particular base station, then the server 27 will request an indication from a HLR of the network 8 of the base station through which the PTD 1 is currently accessing the network 8. In the event that the base station presently serving the PTD 1 corresponds to that defined in the record, then rendering of the corresponding content will be allowed, otherwise the session will be terminated.

In the circumstances where the location restriction is defined by an IP address of an access point, such as a LPRF access point or indeed another PTD, then at least two options exist for determining whether the PTD 1 is in proximity to the access point. In a first alternative, the server 27 contacts the access point and requests location information which it then compares with location information determined for the PTD 1. In a second alternative, the server 27 requests the PTD to authenticate itself to the access point and to provide

evidence of the authentication such that content 29 may then be freely rendered.

In any event, the continued rendering of content 29 is contingent on the restrictions placed in the record file 28 being observed. Thus, the server 27 is obliged to remain satisfied that the conditions for rendering the content 29 remain met. This may not require a full authentication of the PTD 1 but rather only a check to the extent necessary as set by the record 28. Thus, the server 27 will need to repeat at predetermined intervals the process of identifying the location of the PTD 1, for example. To the extent that such information is provided by the PTD 1 itself, in the case of trusted location information, for example, then the digital rights management engine 12 will take part in the process necessary for continued rendering 29 of the content 29. Clearly, once the conditions fail to be met, rendering of the content will be terminated.

The above-described embodiment may be still further understood by reference to the following:

With reference to Figures 2 and hotspot A, in particular, a user of a PTD 1, receives a voucher 11 as part of a promotional exercise carried out by the owner of the fast-food restaurant 18 in conjunction with the operator of the network 8 to which the PTD belongs. The voucher 11 entitles the user to render content 29 in the form of a selection of audio tracks from a recently released album. The voucher 11 is delivered to the PTD 1 by infrared or other suitable point to point connection by the point of sale (POS) equipment (not shown) of the restaurant 18 following the purchase of a pre-determined meal. However, the content record 28 associated with the content 29 held on the secure server 27a under the control of the network 8, includes a location restriction field 31 which permits rendering only within the confines of the restaurant. The restriction is defined in terms of a pico-cell within the network 8 which contains the restaurant 18. As the promotion is for a limited period,

the content record also contains a field 35 indicating the period during which rendering may take place at the specified location. In addition to the voucher 11, the user receives a separate notification to her PTD 1 of the terms of the licence.

The user is able, having purchased the meal to take a seat within the restaurant 13 and request via the UI 4, the content 29 identified in the voucher 11. Accordingly, in response to the request generated via the UI 4 of her PTD 1 and passed by the controller 2 to the digital rights management engine 12, the engine 12 obtains a URL from the voucher 11. The URL provides an address of the secure content server 27a holding the content 29 to which the voucher 11 pertains, namely the selection of audio tracks from a recently released album. The controller 2 having first established a communications channel over the network 8, passes the request to the secure content server 27a together with data indicative of whether the PTD 1 is capable of providing trusted information identifying its physical location.

The server 27a receives the request and commences a handshaking process with the engine 12 contained within the PTD 1. The engine 12 utilises the Public Key Infrastructure (PKI) including those elements held within the voucher 11, namely private keys, to authenticate the voucher 11 and hence the request. If the server 27a is unable to authenticate the voucher 11 then the session is terminated.

Following authentication of the voucher 11, the secure content server 27a seeks to validate the conditions for delivery of the content 29 to the PTD 1 for rendering. The server 27a determines from data provided with the request whether the PTD 1 is capable of providing trusted location information. The server then accesses the record 28 corresponding to the content 29 to be rendered and determines firstly, what limitation if any is placed on a rendering location for the content 29. On finding that the limitation relates to an element of the network 8 namely a base station 17, the server 27 requests an

indication from an HLR 23a of the network 8 of the base station through which the PTD 1 is currently accessing the network 8. In the event that the base station 17 presently serving the PTD 1 corresponds to that defined in the record 28, then rendering of the corresponding content will be allowed, otherwise the session will be terminated.

Subject to any other restrictions on the rendering of the content 29 set out in the record 28, the digital rights management engine 12 of the PTD 1 receives the content 29 which is decrypted thereby and then rendered by the rendering machine 14. An audio output jack on the PTD (not shown) permits the connection of headphones to the device 1 such that the user can enjoy the rendered audio content 29 whilst information relating to the content 29 selected by the user may be presented on the display 5. Should the user leave the confines of the restaurant 18 and thus the scope of the licence conferred by the voucher 11, then as has been previously described the server will stop the rendering of that content.

With reference to Figures 2 and hotspot **B**, in particular, a user of a PTD 1 is pushed details of a sale event at the shopping mall 19. Included with the details is a voucher 11 which entitles the user to render content 29 in the form of various multimedia promotional presentations relating to products available from outlets within the mall 19. However, the content record 28 associated with the content 29 held on the secure server 27a includes a location restriction field 31 pointing to a location database 23b operated by the ISP 25, the database permitting rendering only within the confines of the mall 19. The restriction is defined in terms of a geographical location in the form of the co-ordinates of the mall 19. As the promotion is for a limited period, the content record 28 also contains a field 35 indicating the period during which rendering may take place. In addition to the voucher 11, the user receives a separate notification to her PTD 1 of the terms of the licence.

Having received the voucher 11, the user may choose to travel to the mall 19. On arrival at the mall 19, the user attempts to render the content via the UI 4 and thus a request is passed by the controller 2 to the digital rights management engine 12. The engine 12 obtains a URL from the voucher 11. The URL provides an address of the secure content server 27b holding the content 29 to which the voucher 11 pertains, namely various multimedia promotional presentations relating to products available from outlets within the mall 19. The controller 2 having first established a communications channel over the network 8 to the Internet 16, passes the request to the secure content server 27b together with data indicative of whether the PTD 1 is capable of providing trusted information identifying its physical location.

The server 27b receives the request and commences a handshaking process with the engine 12 contained within the PTD 1. The engine 12 utilises the Public Key Infrastructure (PKI) including those elements held within the voucher 11, namely private keys, to authenticate the voucher 11 and hence the request. If the server is unable to authenticate the voucher 11 then the session is terminated.

Following authentication of the voucher 11, the secure content server 27b seeks to validate the conditions for delivery of the content 29 to the PTD 1 for rendering. The server 27b determines from data provided with the request whether the PTD 1 is capable of providing trusted location information. The server then accesses the record 28 corresponding to the content 29 to be rendered and determines firstly, what limitation if any is placed on a rendering location for the content 29.

On finding that the limitation relates to a location defined by geographical co-ordinates, the server 27b checks whether the PTD 1 is capable of providing trusted location information. If so, a request is issued to the PTD 1 by the server 27b for its co-ordinates. The PTD 1 responds by passing the information on its present location back to the server 27b. Assuming the PTD

1 is appropriately located the server 27b releases the content for rendering by the PTD 1.

If the PTD 1 is not capable of providing trusted location information, then the server 27b must instead form and send a request to the network 8 with which the PTD 1 is associated to provide location information in respect of that PTD 1. How the network 8 determines the location of the PTD 1 in response to such a request will depend on the particular network solution adopted to positioning. Thus, the network 8 may utilise base station triangulation although other suitable techniques will be apparent to those skilled in the art. Once provided and satisfied with the location information relating to the PTD by the network 8, the server 27b is free to release the content for rendering by the PTD 1.

Subject to any other restrictions on the rendering of the content 29 set out in the record 28, the digital rights management engine 12 of the PTD 1 receives the content 29 which is decrypted thereby and then rendered by the rendering machine 14. An audio output jack on the PTD (not shown) permits the connection of headphones to the device such that the user can enjoy the rendered audio content of the presentation whilst video content is presented on the display 5. Should the user leave the confines of the mall and thus the scope of the licence conferred by the voucher 11, then as has been previously described the server 27b will stop the rendering of that content 29.

With reference to Figures 2 and hotspots **C** and **D**, in particular, a doctor may wish to view confidential medical records relating to a patient under her care. The records are located on a secure content server 27c housed within the surgery 20. A storage device 23c holds details relating to the patient location and more particularly; public keys with which an authenticated session may be established with the patients PTD 1.

In accordance with local legislation, the doctor is permitted access to the medical records of her patient within only the confines of her surgery 20 or in the presence of her patient 21. In order to comply with this requirement a record 28 associated with the content 29, namely the medical records of her patient 21, indicates that the content 29 may be rendered in the surgery 20 or in the close proximity **D** to her patient 21. This indication is defined in the first instance by reference to the LPRF access point 26 within the surgery 20 and in the second instance by having the doctor's PTD 1 authenticate itself to the patients PTD 1 by virtue of a short range point to point communication channel, such as LPRF or the like.

The doctor's PTD 1 is pre-loaded with vouchers 11 relating to those patients under her care. In those circumstances where the doctor is present within the surgery 20 and having selected via the UI 4 a particular patient 21 whose records she wish to view, the request is passed by the controller 2 to the digital rights management engine 12. The engine 12 obtains a URL from the voucher 11. The URL provides an address of the secure content server 27a holding the content 29 to which the voucher 11 pertains, namely the medical records of the patient 21. The controller 2 having first established a communications channel over the network 8, passes the request to the secure content server 27c, together with data indicative of whether the PTD 1 is capable of providing trusted information identifying its physical location, in this case its proximity to a patient.

The server 27c receives the request and commences a handshaking process with the engine 12 contained within the PTD 1. The engine 12 utilises the Public Key Infrastructure (PKI) including those elements held within the voucher 11, namely private keys, to authenticate the voucher 11 and hence the request. If the server 27c is unable to authenticate the voucher 11 then the session is terminated.

Following authentication of the voucher 11, the secure content server 27c seeks to validate the conditions for delivery of the content 29 to the PTD 1 for rendering. Thus, the server 27 accesses the record 28 corresponding to the content 29 to be rendered and determines firstly, what limitation if any is placed on a rendering location for the content 29, namely that the PTD 1 is located in the surgery or in proximity to the patient's PTD 1'.

In this case, the server 27c forms part of the surgery management system which includes a LPRF access point 26. Thus, the server 27c is able to query directly the LPRF access point 26 to determine whether the PTD 1 is present within the surgery 20. On finding that the doctor's PTD 1 is within the surgery 20, the content 29 is delivered for rendering to the PTD 1. To provide additional security, the content 29 may be delivered over the LPRF access point 26 rather than using the network 8. Indeed the whole process of seeking access to the content 29 by the PTD 1 may, instead of utilising the network 8, be carried out via the LPRF access point 26. Subject to any other restrictions on the rendering of the content 29 set out in the record 28, the digital rights management engine 12 of the PTD 1 receives the content 29 which is decrypted thereby and then rendered by the rendering machine 14. As before, should the doctor leave the confines of the surgery 20 and thus the scope of the licence conferred by the voucher 11, then as has been previously described, the server 27c will stop the rendering of that content 29 on the PTD 1.

In the event that the doctor is with the patient 21 outside of the surgery 20, then the request for rendered content 29 namely the medical records of the patient 21 is passed by the controller 2 to the digital rights management engine 12. The engine 12 obtains a URL from the voucher 11. The URL provides an address of the secure content server 27 holding the content 29 to which the voucher 11 pertains, namely the medical records of the patient 21. The controller 2 having first established a communications channel over the network 8, passes the request to the secure content server 27c together with

data indicative of whether the PTD 1 is capable of providing trusted information identifying its physical location, in this case its proximity to a patient.

The server 27c receives the request and commences a handshaking process with the engine 12 contained within the PTD 1. The engine 12 utilises the Public Key Infrastructure (PKI) including those elements held within the voucher 11, namely private keys, to authenticate the voucher 11 and hence the request. If the server 27c is unable to authenticate the voucher 11 then the session is terminated.

Following authentication of the voucher 11, the secure content server 27c seeks to validate the conditions for delivery of the content 29 to the PTD 1 for rendering. Thus, the server 27 accesses the record 28 corresponding to the content 29 to be rendered and determines firstly, what limitation if any is placed on a rendering location for the content 29, namely that the PTD 1 is located in the surgery 20 or in proximity to the patient's PTD 1'.

As has been set out above, the server 27c forms part of the surgery management system which includes the LPRF access point 26. Thus, the server 27c is able to query directly the LPRF access point 26 to determine whether the PTD 1 is present within the surgery 20. On finding that the doctor's PTD 1 is not within the surgery 20, the server 27c issues a request over the network 8 to the doctor's PTD 1 to authenticate itself to the patients PTD 1'. On receiving the request, the digital rights management engine 12 initiates a suitable authentication process over a LPRF connection (not shown) to the patient's PTD 1'. Successful completion of the process results in an appropriate response being made to the server 27c. Clearly, the response to the server 27c should include elements of the PKI which will assure the server 27c that the doctor's PTD 1 is properly authenticated and therefore in proximity to the patients device 1'. Subsequently, and subject to any other restrictions on the rendering of the content 29 set out in the record

28, the content 29 is delivered over the network 8 to the doctor's PTD 1 for rendering thereby. The digital rights management engine 12 of the PTD 1 receives the content 29 which is decrypted thereby and then rendered by the rendering machine 14 for presentation by a suitable element such as the displays. Should the doctor leave the proximity of the patient's PTD 1' and thus the scope of the licence conferred by the voucher 11, then as has been previously described, the updates of the location of the PTD 1 demanded by the server 27c will reveal this event and the server 27c will terminate the rendering of that content.

It will be readily apparent from the above that many of the processes involved in rendering content on the PTD 1 depend on the provision of confidential or personal information particularly relating to location finding. Thus, various forms of encryption may put in place to protect both information and channels of communication over which such information is transferred.

Claims:

1. A content delivery system for securely rendering content on a terminal, the system comprising a mobile terminal operable to establish a connection to a network and request delivery of content from a secure content server, said network being operable to determine the location of said terminal and provide access to said secure content server, the server being operable to associate said content identified in said request with at least one delivery condition stored on a database, a said at least one delivery condition defining a rendering location, the server being further operable to obtain the location of the terminal from said network such that where said terminal location corresponds to said rendering location content is delivered to said terminal.

2. A system as claimed in Claim 1, wherein said terminal includes a rendering machine.

3. A system as claimed in Claim 1 or Claim 2, wherein the content is delivered to said terminal over the network.

4. A content delivery system for securely rendering content on a terminal, the system comprising a mobile terminal operable to determine its location and to establish a connection to a network in order to request delivery of content from a secure content server, said network being operable to provide access to said secure content server, the server being operable to associate said content identified in said request with at least one delivery condition stored on a database, a said at least one delivery condition defining a rendering location, the server being further operable to obtain the location of the terminal from said terminal such that where said terminal location corresponds to said rendering location content is delivered to said terminal.

5. A system as claimed in Claim 5, in which the network is operable to determine the location of said terminal such that the server selectably obtains the location of the terminal from the network.

6. A system as claimed in Claim 4 or Claim 5, wherein said terminal includes a rendering machine.

7. A system as claimed in any one of Claims 4 to 6, wherein the content is delivered to said terminal over the network.

8. A system as claimed in any preceding Claim, wherein the content is stored on said database.

9. A system as claimed in Claim 8, wherein the content includes said condition as metadata.

10. A system as claimed in any preceding Claim, wherein the database is accessed via a network.

11. A content delivery system for securely rendering content on a terminal, the system comprising a mobile terminal operable to determine its location and to establish a connection to an access point in order to request delivery of content from a secure content server, said access point being operable to provide access to said secure content server, the server being operable to associate said content identified in said request with at least one delivery condition stored on a database, a said at least one delivery condition defining a rendering location, the server being further operable to obtain the location of the terminal from said access point such that where said terminal location corresponds to said rendering location content is delivered to said terminal.

12. A system as claimed in Claim 11, wherein the access point is connected to the server via a network.

13. A system as claimed in Claim 12, wherein the network is a wireless network.

14. A system as claimed in any one of Claims 11 to 13, wherein said terminal includes a rendering machine.

15. A system as claimed in any one of Claims 11 to 14, wherein the content is delivered to said terminal over a network.

16. A system as claimed in any one of Claims 11 to 15, wherein the content is stored on said database.

17. A system as claimed in Claim 16, wherein the content includes said condition as metadata.

18. A system as claimed in any one of Claims 11 to 17, wherein the database is accessed via a network.

19. A content delivery system for securely rendering content on a terminal, the system comprising a mobile terminal operable to establish a connection to an access point in order to request delivery of content from a secure content server, said access point being operable to provide access to said secure content server, the server being operable to associate said content identified in said request with at least one delivery condition stored on a database, a said at least one delivery condition defining a rendering location, the server being further operable to obtain the location of the terminal such that where said terminal location corresponds to said rendering location content is delivered to said terminal.

20. A system as claimed in Claim 19, wherein the access point is connected to the server via a network.

21. A system as claimed in Claim 20, wherein the network is a wireless network.

22. A system as claimed in any one of Claims 19 to 21, wherein said terminal includes a rendering machine.

23. A system as claimed in any one of Claims 19 to 22, wherein the content is delivered to said terminal over a network.

24. A system as claimed in any one of Claims 19 to 23, in which the access point is operable to determine the location of said terminal such that the server selectably obtains the location of the terminal from the access point.

25. A system as claimed in any one of Claims 19 to 24, wherein the content is stored on said database.

26. A system as claimed in Claim 25, wherein the content includes said condition as metadata.

27. A system as claimed in any one of Claims 19 to 26, wherein the database is accessed via a network.

28. A secure content server including a database having stored thereon at least one delivery condition associated with content, the server being operable in response to a request for content from a terminal to determine from said database a said at least one delivery condition defining a rendering location of said content, the server being further operable to obtain the location of the terminal such that where said

terminal location corresponds to said rendering location said content is delivered to said terminal.

29. A server as claimed in Claim 28, wherein the content is stored on said database.

30. A server as claimed in Claim 29, wherein the content includes said condition as metadata.

31. A server as claimed in any one of Claims 28 to 30, wherein the database is accessed via a network.

32. A content delivery method for securely rendering content on a terminal, the method comprising receiving a request from a terminal for delivery of content, associating said content identified in said request with at least one delivery condition stored on a database, a said at least one delivery condition defining a rendering location, obtaining the location of the terminal and delivering said content to said terminal where said terminal location corresponds to said rendering location.

33. A computer program comprising executable code for execution when loaded on a computer, wherein the computer is operable in accordance with said code to carry out the method according to Claim 32.

34. A program as claimed in Claim 33, stored in a computer readable medium.

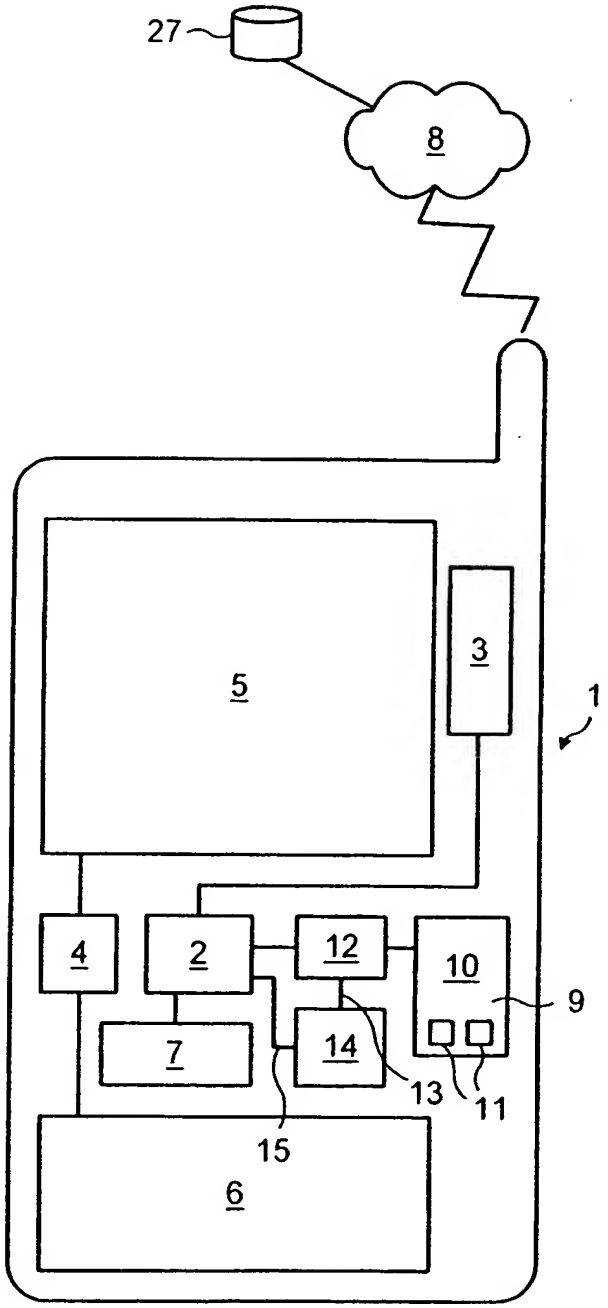


FIG. 1

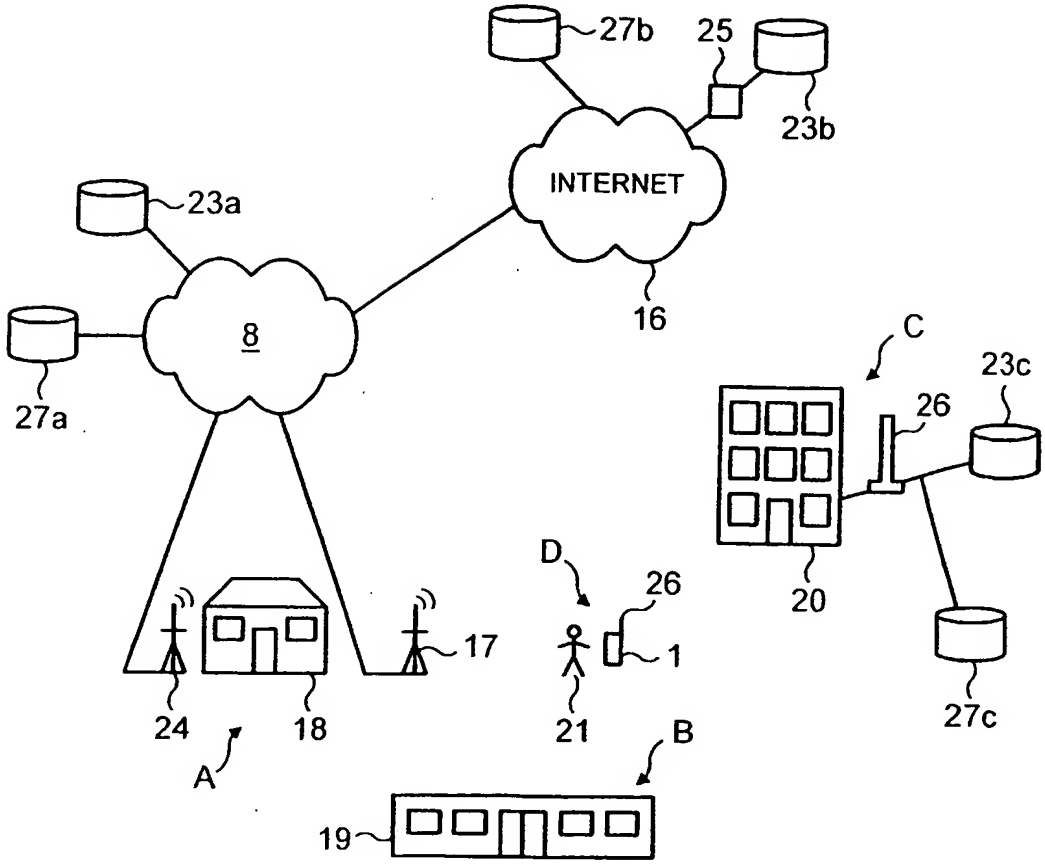

27b
25
23b
INTERNET
23a
16
8
27a
C
23c
26
20
27c
D
26
1
17
24
18
21
A
B
19

FIG. 2

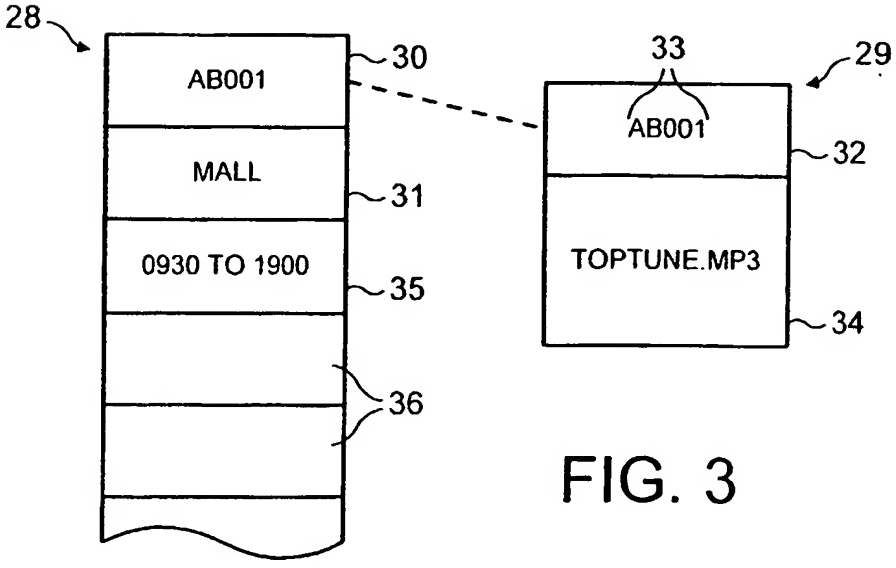

28
AB001
30
MALL
31
0930 TO 1900
35
36
33
29
AB001
32
TOPTUNE.MP3
34

FIG. 3

PCT/EP 01/08292

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 G06F17/60 G06F17/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 99 55102 A (ISRAELI GIL ;TE ENI BEN (IL); NETLINE COMMUNICATIONS TECHNOL (IL)) 28 October 1999 (1999-10-28) abstract page 11, line 4 - line 10 page 12, line 27 -page 13, line 20 page 14, line 10 -page 15, line 6 page 16, line 4 - line 10 claims 1,10 --- -/--	1-34

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 June 2002	11/06/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Karavassilis, N

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	WO 99 51038 A (PICCIONELLI GREG A ;RITTMASTER TED R (US)) 7 October 1999 (1999-10-07) abstract page 2, line 25 -page 4, line 9 page 6, line 6 - line 35 page 11, line 17 -page 12, line 15 page 14, line 25 -page 16, line 8 page 20, line 27 -page 21, line 33 claim 1 ---	1-34
X	EP 0 853 287 A (NOKIA MOBILE PHONES LTD) 15 July 1998 (1998-07-15) page 3, column 3, line 20 -column 4, line 8 page 5, column 7, line 37 -column 8, line 4 page 8, column 14, line 56 -page 9, column 15, line 48 ---	1-34
P,X	EP 1 077 437 A (PHONE COM INC) 21 February 2001 (2001-02-21) abstract page 2, column 2, line 6 -page 5, column 7, line 19 page 6, column 10, line 32 -page 8, column 13, line 37 ---	1-34
E	US 6 332 127 B1 (BANDERA DANIEL QUINTO ET AL) 18 December 2001 (2001-12-18) abstract column 3, line 19 - line 43 column 9, line 47 -column 10, line 51 -----	1-34

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9955102 A	28-10-1999	AU 3343799 A	08-11-1999
		EP 1074156 A1	07-02-2001
		WO 9955102 A1	28-10-1999
WO 9951038 A	07-10-1999	US 6154172 A	28-11-2000
		AU 3217299 A	18-10-1999
		CN 1330770 T	09-01-2002
		EP 1090307 A2	11-04-2001
		JP 2002510814 T	09-04-2002
		WO 9951038 A2	07-10-1999
EP 0853287 A	15-07-1998	FI 965278 A	01-07-1998
		CA 2225191 A1	30-06-1998
		EP 0853287 A2	15-07-1998
		JP 10257100 A	25-09-1998
		US 6154745 A	28-11-2000
EP 1077437 A	21-02-2001	CN 1280344 A	17-01-2001
		EP 1077437 A2	21-02-2001
		JP 2001076058 A	23-03-2001
US 6332127 B1	18-12-2001	JP 2000222331 A	11-08-2000